



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

December 09, 2014

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:

SA2014-087

DATE(S) ISSUED:

12/09/2014

SUBJECT:

Vulnerabilities in Microsoft Word and Microsoft Office Web Apps Could Allow Remote Code Execution (MS14-081)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Word and Microsoft Web Apps that could allow an attacker to take complete control of an affected system. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

There are currently no reports of this vulnerability being exploited in the wild.

SYSTEM AFFECTED:

- Microsoft Office 2007 Service Pack 3
- Microsoft Office 2010 Service Pack 2 (32-bit editions)
- Microsoft Office 2010 Service Pack 2 (64-bit editions)
- Microsoft Office 2013 (32-bit editions)
- Microsoft Office 2013 Service Pack 1 (32-bit editions)
- Microsoft Office 2013 (64-bit editions)
- Microsoft Office 2013 Service Pack 1 (64-bit editions)
- Microsoft Office 2013 RT
- Microsoft Office 2013 RT Service Pack 1
- Microsoft Office for Mac 2011
- Microsoft Word Viewer
- Microsoft Office Compatibility Pack Service Pack 3
- Microsoft SharePoint Server 2010 Service Pack 2
- Microsoft SharePoint Server 2013
- Microsoft SharePoint Server 2013 Service Pack 1
- Microsoft Office Web Apps 2010 Service Pack 2
- Microsoft Office Web Apps 2013
- Microsoft Office Web Apps 2013 Service Pack 1

RISK:**Government:**

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Two memory corruption vulnerabilities have been discovered that could allow for remote code execution. The vulnerabilities exist due to Microsoft Word not properly handling objects in memory while parsing specially crafted Office files.

These vulnerabilities can be exploited by opening a specially crafted file and can be exploited via email or through the web. In the email-based scenario, the user would have to open the specially crafted file as an email attachment. In the web based scenario, a user would have to open the specially crafted file that is hosted on a website. The attacker-supplied code would then execute if the user opens the file using Microsoft Office.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:**Microsoft:**

<https://technet.microsoft.com/library/security/ms14-081>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6356>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6357>